PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-251006
(43)Date of publication of application : 14.09.2000

(51)Int.Cl. G06F 19/00
G06F 12/14
G09C 1/00
H04L 9/32

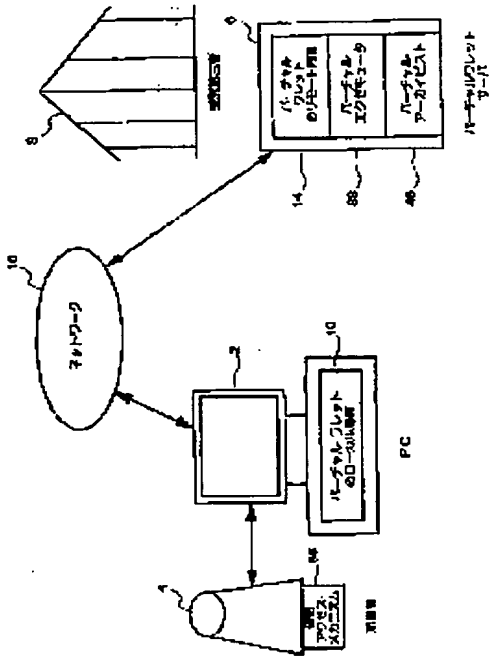
(21)Application number : 11-106664
(22)Date of filing : 14.04.1999

(71)Applicant : CITICORP DEV CENTER INC
(72)Inventor : PALTENGHE CRIS T
MAMDANI ALNOR B
EZROL LISA
GOLVIN CHARLES
HENRY RIKUSUTEN
TAKATA MELVIN MICHIO

(30)Priority
Priority number : 98 81748 Priority date : 14.04.1998 Priority country : US
98 190993 12.11.1998 US

(54) SYSTEM AND METHOD FOR SAFELY STORING ELECTRONIC DATA

(57)Abstract:
PROBLEM TO BE SOLVED: To prepare access to stored data for the third person of a trustee in the occurrence of an event such as the death of an owner by storing, managing and updating the secret data of the owner.
SOLUTION: This system uses the application software of a virtual wallet 6 which is executed on the server of the third person of the trustee and provided with a virtual executor 38 and a virtual archivist 46. When accessing the stored data, the virtual executor 38 automatically escrows the access stage of the third person of the trustee of a secret device for the owner. When the occurrence of a conditional event is confirmed, the virtual executor 38 provides access to the stored data while using the access stage of the third person of the trustee. The virtual archivist 46 automatically updates techniques related to the stored data.



(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号

特開２０００－２５１００６
（Ｐ２０００－２５１００６Ａ）
(43)公開日　平成12年9月14日(2000.9.14)

(51)Int.Cl.[7]	識別記号	FI		テーマコード(参考)
Ｇ０６Ｆ　19/00		Ｇ０６Ｆ　15/30	Ｚ	
12/14	３２０	12/14	３２０　Ａ	
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０　Ｚ	
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３　Ｄ	

審査請求　未請求　請求項の数１　ＯＬ　外国語出願　（全３９頁）

(21)出願番号　特願平11-106664

(22)出願日　平成11年4月14日(1999.4.14)

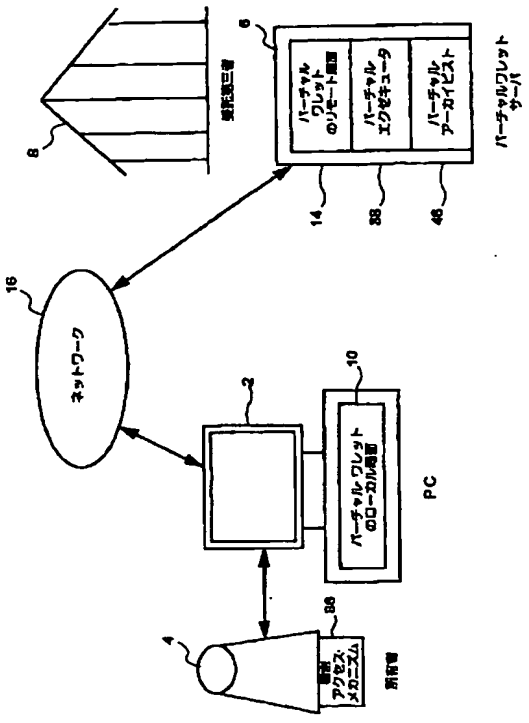
(31)優先権主張番号　60/081748
(32)優先日　平成10年4月14日(1998.4.14)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　09/190993
(32)優先日　平成10年11月12日(1998.11.12)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　598156527
シティコープ　デヴェロップメント　センター，インコーポレイテッド
Ｃｉｔｉｃｏｒｐ　Ｄｅｖｅｌｏｐｍｅｎｔ　Ｃｅｎｔｅｒ，Ｉｎｃ．
アメリカ合衆国　カリフォルニア州　90066，ロスアンジェルス，ダヴリュー．ジェファーソン　ブールバード　12731
(74)代理人　100092956
弁理士　古谷　栄男　（外3名）

最終頁に続く

(54)【発明の名称】電子データを安全に蓄積するためのシステムおよび方法

(57)【要約】　（修正有）
【課題】所有者の機密データを蓄積して管理し、更新する。所有者の死亡のような事象の発生時に受託第三者による蓄積データへのアクセスに備える。
【解決手段】受託第三者のサーバ上で実行され、またバーチャル・エクゼキュータ３８およびバーチャル・アーカイビスト４６を備えるバーチャルワレット６のアプリケーションソフトウェアを使用する。バーチャル・エクゼキュータ３８は、蓄積データにアクセスするにあたって、所有者のための機密装置の受託第三者のアクセス局面を自動的にエスクローする。条件事象の発生が確認されると、バーチャル・エクゼキュータ３８は、受託第三者のアクセス局面を用いて、蓄積データへのアクセスを提供する。バーチャル・アーカイビスト４６は、蓄積データに関連する技術を自動的に更新する。



1

【特許請求の範囲】

【請求項１】所有者のためにデータを安全に蓄積するための方法であって：前記所有者のために前記データを蓄積するステップ；前記蓄積データへアクセスするために、機密装置を前記所有者に自動的に割り当てるステップ；事象の発生時に条件づけられる前記機密装置を自動的にエスクローするステップ；前記事象の発生の確認を受け取るステップ；および、前記エスクローされた機密装置を用いて、前記蓄積データにアクセスするステップ；を含む方法。

【請求項２】前記データを蓄積するステップが、前記所有者のためにバーチャルワレット・アプリケーション上で前記データを入力するステップを更に含む、請求項１の方法。

【請求項３】前記データを蓄積するステップが、端末で、前記所有者が前記データを入力するステップを更に含む、請求項２の方法。

【請求項４】前記データを入力するステップが、サーバに結合されている前記端末で、前記所有者が前記データを入力するステップを更に含む、請求項３の方法。

【請求項５】前記端末がパソコンを更に備える、請求項４の方法。

【請求項６】前記サーバが、受託第三者のサーバを更に備える、請求項４の方法。

【請求項７】前記受託第三者の前記サーバが金融機関サーバを更に備える、請求項６の方法。

【請求項８】前記金融機関が銀行を更に含む、請求項７の方法。

【請求項９】前記データを入力するステップが、ネットワーク上の前記サーバに結合されている前記端末で、前記所有者が前記データを入力するステップを更に含む、請求項４の方法。

【請求項１０】前記ネットワークが専用回線を更に含む、請求項９の方法。

【請求項１１】前記ネットワークが公衆回線を更に含む、請求項９の方法。

【請求項１２】前記公衆回線がインターネットを更に含む、請求項１１の方法。

【請求項１３】前記データを入力するステップが、バーチャル・エクゼキュータ機能を持つバーチャルワレット・アプリケーション上で前記所有者のために前記データを入力するステップを更に含む、請求項２方法。

【請求項１４】前記データを入力するステップが、バーチャル・アーカイビスト機能を持つバーチャルワレット・アプリケーション上で前記所有者のために前記データを入力するステップを更に含む、請求項２方法。

【請求項１５】前記データを蓄積するステップが、端末で前記所有者が前記データを入力するステップを更に含む、請求項１方法。

【請求項１６】前記端末がパソコンを更に備える、請求項１５の方法。

2

【請求項１７】前記データを入力するステップが、サーバに結合されている前記端末で、前記所有者が前記データを入力するステップを更に含む、請求項１５の方法。

【請求項１８】前記データを入力するステップが、前記サーバ上に少なくとも一部が在住する前記データを、バーチャルワレット・アプリケーション上で入力するステップを更に含む、請求項１７の方法。

【請求項１９】前記データを入力するステップが、前記端末上に少なくとも一部が在住する前記データを、バーチャルワレット・アプリケーション上で入力するステップを更に含む、請求項１７の方法。

【請求項２０】前記データを入力するステップが、識別情報、認証情報、証明書情報、アクセス・キー情報、ＰＩＮ番号情報、クレジットカード口座情報、デビットカード情報、銀行口座情報、および他の個人情報から成る一群の情報から選択された少なくとも１つのカテゴリの情報を、前記所有者のためにバーチャルワレット・アプリケーションにより蓄積するステップを更に含む、請求項１の方法。

【請求項２１】前記機密装置を割り当てるステップが、バーチャルワレット・アプリケーションにより前記所有者へ前記機密装置を割り当てるステップを更に含む、請求項１の方法。

【請求項２２】前記機密装置を自動的に割り当てるステップが、端末で前記所有者へ前記機密装置を自動的に割り当てるステップを更に含む、請求項２１の方法。

【請求項２３】前記機密装置を自動的に割り当てるステップが、前記端末に結合されているサーバ上に少なくとも一部が在住する前記機密装置を、前記バーチャルワレット・アプリケーションにより自動的に割り当てるステップを更に含む、請求項２２の方法。

【請求項２４】前記端末がパソコンを更に備える、請求項２３の方法。

【請求項２５】前記サーバが、受託第三者の前記サーバを更に備える、請求項２３の方法。

【請求項２６】前記受託第三者の前記サーバが、金融機関サーバを更に含む、請求項２５の方法。

【請求項２７】前記金融機関が銀行を更に含む、請求項２６の方法。

【請求項２８】前記機密装置を自動的に割り当てるステップが、ネットワーク上で前記サーバに結合されている前記端末で前記機密装置に関する情報を、前記所有者へ自動的に送るステップを更に含む、請求項２３の方法。

【請求項２９】前記ネットワークが専用回線を更に含む、請求項２８の方法。

【請求項３０】前記ネットワークが公衆回線を更に含む、請求項２８の方法。

【請求項３１】前記公衆回線がインターネットを更に含む、請求項３０の方法。

【請求項３２】前記機密装置を自動的に割り当てるステップが、少なくとも２つのアクセス局面で前記機密装置を自動的に割り当てるステップを更に含む、請求項１の方法。

【請求項３３】前記機密装置を自動的に割り当てるステップが、所有者のアクセス局面と受託第三者のアクセス局面とへ、前記機密装置を自動的に割り当てるステップを更に含む、請求項３２の方法。

【請求項３４】前記所有者のアクセス局面を自動的に割り当てるステップが、前記所有者へ前記所有者のアクセス局面を自動的に送るステップを更に含む、請求項３３の方法。

【請求項３５】前記受託第三者のアクセス局面を自動的に割り当てるステップが、前記受託第三者のアクセス局面を自動的に蓄積するステップを更に含む、請求項３３の方法。

【請求項３６】前記受託第三者のアクセス局面を自動的に蓄積するステップが、バーチャルワレット・アプリケーションにより、前記所有者のために前記受託第三者のアクセス局面を自動的に蓄積するステップを更に含む、請求項３５の方法。

【請求項３７】前記受託第三者のアクセス局面を自動的に蓄積するステップが、前記バーチャルワレット・アプリケーションのバーチャル・エクゼキュータ機能により、前記所有者のために前記受託第三者のアクセス局面を自動的に蓄積するステップを更に含む、請求項３６の方法。

【請求項３８】前記受託第三者のアクセス局面を自動的に蓄積するステップが、前記受託第三者のサーバ上で前記バーチャルワレット・アプリケーションの前記バーチャル・エクゼキュータ機能により、前記受託第三者のアクセス局面を自動的に蓄積するステップを更に含む、請求項３７の方法。

【請求項３９】前記受託第三者のサーバが、金融機関のコンピュータを更に備える、請求項３８の方法。

【請求項４０】前記金融機関が銀行を更に含む、請求項３９の方法。

【請求項４１】前記機密装置を自動的にエスクローするステップが、前記機密装置の受託第三者のアクセス局面を、前記所有者のために自動的にエスクローするステップを更に含む、請求項１の方法。

【請求項４２】前記受託第三者のアクセス局面を自動的にエスクローするステップが、バーチャルワレット・アプリケーションにより、前記受託第三者のアクセス局面を、前記所有者のために自動的に蓄積するステップを更に含む、請求項４１の方法。

【請求項４３】前記受託第三者のアクセス局面を自動的に蓄積するステップが、前記バーチャルワレットのバーチャル・エクゼキュータ機能により、前記受託第三者のアクセス局面を自動的に蓄積するステップを更に含む、請求項４２の方法。

【請求項４４】前記受託第三者のアクセス局面を自動的にエスクローするステップが、前記所有者に影響を及ぼす事象の発生時に条件づけられている前記受託第三者のアクセス局面を自動的に蓄積するステップを更に含む、請求項４１の方法。

【請求項４５】前記所有者に影響を及ぼす前記事象が、前記所有者の死亡を含む、請求項４４の方法。

【請求項４６】前記所有者に影響を及ぼす前記事象が、前記所有者の資格喪失を含む、請求項４４の方法。

【請求項４７】前記機密装置を自動的にエスクローするステップが、前記所有者のために機密アクセス情報を自動的にエスクローするステップを更に含む、請求項１の方法。

【請求項４８】機密アクセス情報を自動的にエスクローするステップが、識別情報、認証情報、証明書情報、アクセス・キー情報、ＰＩＮ番号情報、およびパスワード情報、から成る一群の機密アクセス情報から選択された少なくとも１つのタイプの機密アクセス情報を自動的に蓄積するステップを更に含む、請求項４７の方法。

【請求項４９】前記機密装置を自動的にエスクローするステップが、前記所有者のために暗号解読インフラを自動的にエスクローするステップを更に含む、請求項１の方法。

【請求項５０】暗号解読インフラを自動的にエスクローするステップが、公開キー暗号手法インフラ、電子文書インフラ、デジタル署名インフラ、ユーザー名・インフラ、パスワード・インフラ、指紋スキャナ・インフラ、および機密キー・インフラから成る一群の暗号解読インフラから選択された少なくとも１つの暗号解読インフラを自動的に蓄積するステップを更に含む、請求項４９の方法。

【請求項５１】前記確認を受け取るステップが、受託第三者により前記所有者のために確認を受け取るステップを更に含む、請求項１の方法。

【請求項５２】前記確認を受け取るステップが、前記所有者の個人代理人から前記確認を受け取るステップを更に含む、請求項１の方法。

【請求項５３】前記確認を受け取るステップが、前記所有者に影響を及ぼす事象の前記確認を受けるステップを更に含む、請求項１の方法。

【請求項５４】前記所有者に影響を及ぼす前記事象が、前記所有者の死亡を更に含む、請求項５３の方法。

【請求項５５】前記所有者に影響を及ぼす前記事象が、前記所有者の資格喪失を更に含む、請求項５３の方法。

【請求項５６】前記確認を受け取るステップが、前記所有者のバーチャルワレット・アプリケーション上で前記事象の発生の確認を入力するステップを更に含む、請求項１の方法。

【請求項５７】前記確認を入力するステップが、前記バ

ーチャルワレット・アプリケーションのバーチャル・エクゼキュータ機能上で前記確認を入力するステップを更に含む、請求項５６の方法。

【請求項５８】前記確認を入力するステップが、サーバ上の前記バーチャルワレット・アプリケーションの前記バーチャル・エクゼキュータ機能上で、前記確認を入力するステップを更に含む、請求項５６の方法。

【請求項５９】前記確認を入力するステップが、受託第三者のサーバ上の前記バーチャルワレット・アプリケーションの前記バーチャル・エクゼキュータ機能上で、前記確認を入力するステップを更に含む、請求項５８の方法。

【請求項６０】前記受託第三者が金融機関を更に含む、請求項５９の方法。

【請求項６１】前記金融機関が銀行を更に含む、請求項６０の方法。

【請求項６２】前記蓄積データにアクセスするステップが、前記所有者のバーチャルワレット・アプリケーションに蓄積されている前記データにアクセスするステップを更に含む、請求項１の方法。

【請求項６３】前記蓄積データにアクセスするステップが、サーバ上のバーチャルワレット・アプリケーションのバーチャル・エクゼキュータ機能に蓄積されている前記データにアクセスするステップを更に含む、請求項６２の方法。

【請求項６４】前記蓄積データにアクセスするステップが、受託第三者の前記サーバ上の前記バーチャルワレット・アプリケーションの前記バーチャル・エクゼキュータ機能に蓄積されている前記データにアクセスするステップを更に含む、請求項６３の方法。

【請求項６５】前記受託第三者が金融機関を更に含む、請求項６４の方法。

【請求項６６】前記金融機関が銀行を更に含む、請求項６５の方法。

【請求項６７】前記蓄積データへアクセスするステップが、前記機密装置の受託第三者のアクセス局面を用いて前記データへアクセスするステップを更に含む、請求項１の方法。

【請求項６８】前記データへアクセスするステップが、バーチャルワレット・アプリケーションのバーチャル・エクゼキュータ機能により蓄積されている前記機密装置の前記受託第三者のアクセス局面を用いて、前記データにアクセスするステップを更に含む、請求項６７の方法。

【請求項６９】前記データにアクセスするステップが、前記受託第三者のサーバ上の前記バーチャルワレット・アプリケーションの前記バーチャル・エクゼキュータ機能により蓄積されている前記機密装置の前記受託第三者のアクセス局面を用いて、前記データにアクセスするステップを更に含む、請求項６８の方法。

【請求項７０】前記受託第三者が金融機関を更に含む、請求項６９の方法。

【請求項７１】前記金融機関が銀行を更に含む、請求項７０の方法。

【請求項７２】前記蓄積データの技術局面を自動的に更新するステップを更に含む、請求項１の方法。

【請求項７３】前記技術局面を自動的に更新するステップが、バーチャルワレット・アプリケーションのバーチャル・アーカイビスト機能により、前記データの技術局面を自動的に更新するステップを更に含む、請求項７２の方法。

【請求項７４】前記バーチャル・アーカイビスト機能により前記技術局面を自動的に更新するステップが、サーバ上の前記バーチャルワレット・アプリケーションの前記バーチャル・アーカイビスト機能により、前記技術局面を自動的に更新するステップを更に含む、請求項７３の方法。

【請求項７５】前記技術局面を自動的に更新するステップが、受託第三者の前記サーバ上の前記バーチャルワレット・アプリケーションの前記バーチャル・アーカイビスト機能により、前記技術局面を自動的に更新するステップを更に含む、請求項７４の方法。

【請求項７６】前記受託第三者が金融機関を更に含む、請求項７５の方法。

【請求項７７】前記金融機関が銀行を更に含む、請求項７６の方法。

【請求項７８】前記技術局面を自動的に更新するステップが、文書署名に関連する技術、暗号化技術、文書署名のためのキーに関連する技術、文書自体に関連する技術、証明書取消しリストに関連する技術、時間スタンプに関連する技術および公証人スタンプに関連する技術から成る一群の技術局面から選択された、前記データの少なくとも１つの技術局面を自動的に更新するステップを更に含む、請求項１の方法。

【請求項７９】前記データを蓄積するステップが、前記所有者のためにバーチャルワレット・アプリケーションにより別の当事者から前記データを受け取るステップを更に含む、請求項１の方法。

【請求項８０】前記データを受け取るステップが、電子メールを介して、前記所有者のために前記バーチャルワレット・アプリケーションにより前記データを受け取るステップを更に含む、請求項７９の方法。

【請求項８１】所有者のためにデータを安全に蓄積するためのシステムであって：前記所有者のために前記データを蓄積するための手段；前記蓄積データにアクセスするために前記所有者に機密装置を自動的に割り当てるための、前記蓄積手段に関連する手段；事象の発生時に条件づけられた前記機密装置を自動的にエスクローするための、前記蓄積手段に関連する手段；前記事象の発生の確認を受け取るための、前記蓄積手段に関連する手段；

および、前記エスクローされた機密装置を用いて前記蓄積データにアクセスするための、前記蓄積手段に関連する手段；を備えるシステム。

【請求項８２】前記データを蓄積するための前記手段が、サーバを更に備える、請求項８１のシステム

【請求項８３】前記サーバが、受託当事者の前記サーバを更に備える、請求項８２のシステム。

【請求項８４】前記データを蓄積するための前記手段が、前記サーバへされている端末を更に備える、請求項８３のシステム。

【請求項８５】前記データを蓄積するための前記手段が、前記端末を前記サーバへ結合するネットワークを更に備える、請求項８４のシステム。

【請求項８６】前記機密装置を自動的に割り当てるための前記手段が、サーバを更に備える、請求項８１のシステム。

【請求項８７】前記サーバが、受託第三者の前記サーバを更に備える、請求項８６のシステム。

【請求項８８】前記機密装置を自動的に割り当てるための前記手段が、ネットワーク上の端末に結合されている前記サーバを更に備える、請求項８１のシステム。

【請求項８９】前記確認を受け取るための前記手段が、サーバを更に備える、請求項８１のシステム。

【請求項９０】前記サーバが、受託第三者の前記サーバを更に備える、請求項８９のシステム。

【請求項９１】前記蓄積データにアクセスするための前記手段が、サーバを更に備える、請求項８１のシステム。

【請求項９２】前記サーバが、受託第三者の前記サーバを更に備える、請求項９１のシステム。

【発明の詳細な説明】

【関連特許出願とのクロスリファレンス】本出願は、引用して本明細書に組込まれている、１９９８年４月１４日出願の米国仮特許出願第６０／０８１，７４８号；１９９８年１１月１２日出願の同時係属中米国特許出願第０９／１９０、９９３号；＿＿＿年＿月＿＿日出願の「インターネット・ウェブサイトへの蓄積情報伝送を制御するためのシステムおよび方法」と題する特許出願第＿＿＿＿＿＿号；および＿＿＿年＿月＿＿日出願の「デジタルグラフィック署名システム」と題する特許出願第＿＿＿＿＿＿号；の恩典を請求する。

【発明の分野】本発明は、一般的に電子データの蓄積に関し、より詳細には所有者のデータを安全に蓄積、管理、更新するための、そして所有者の死亡などの事象の発生時、蓄積データへ受託当事者がアクセスするためのシステムと方法に関する。

【発明の背景】電子的な、あるいはバーチャルなワレットは、電子オブジェクト、例えば所有者のペイメント・メカニズム、アイデンティティ認証メカニズム、個人情報、およびアーチファクトなどのための容器として働らくソフトウェアの一実施形態である。電子的な、あるいはバーチャルなワレットは、例えば、コンシューマのパソコン（ＰＣ）、サーバ、およびスマートカードの何れかひとつ以上に在住できる。バーチャルワレットは、所有者がワレット内の情報へのアクセス、および情報の分配を可能にし、それにより所有者の個人情報に対する所有者のセキュリティと全体的コントロールが得られる。更に、バーチャルワレットは、例えば、ワレットの内容を遠隔地(remotely)から蓄積および／またはディスエーブル化することにより、ワレット内の情報の損失リスクを解消するメカニズムを提供する。従ってバーチャルワレットは、情報や価値を持つ金融品を保持するための受託場所であり、また情報を動き巡らせる便利な方法である。現在、電子ワレットの多くは、ペイメント・メカニズム（支払いメカニズム）に焦点を当てている。しかし電子ワレットを用いて、例えば識別情報、認証情報、証明書、アクセス・キー、個人識別番号（ＰＩＮ）、およびクレジットカード／デビットカード／銀行口座情報、並びに所有者の遺言書など他のすべてのタイプの個人情報を保存することもできる。電子的な、あるいはバーチャルなワレットの詳細な検討に関しては、例えば引用して本明細書に組込まれている、１９９８年４月１４日出願の、現在、同時係属中である仮特許出願第６０／０８１，７４８号、および１９９８年１１月１２日出願の特許出願第０９／１９０，９９３号を参照されたい。電子ワレット中に蓄積されている情報は、電子ワレットの所有者により、例えばインターネットまたは他のタイプのネットワークを介して伝送されるとともに受け取られる。通常、バーチャルワレットのローカル局面は、所有者のパソコン（ＰＣ）上に在住し、所有者が、例えばサーバ上に在住するバーチャルワレット全体へ遠隔地からのアクセス権を獲得することを可能にする証明書または他の類似認証書類を含む。バーチャルワレットのこのローカル局面は、ローカルワレットがオンライン状態にあるとき、ローカル局面からの最新情報を用いて、バーチャルワレットのリモート（遠隔）局面を更新する。またサーバは、例えば所有者のＰＣよりも大きな蓄積容量を、所有者の情報のために提供する。従って所有者は、ワレットのリモート局面がワレット内に蓄積されている情報の全てにセキュリティを提供する一方で、ワレットのローカル局面がサーバにリンクされ得るサイトでのワレット機能全体を定義して、そこへのアクセス権を持つことができる。しかし、バーチャルワレット内に安全に蓄積されている所有者の電子データへのアクセス権を所有者が獲得することを可能にする特定のＰＩＮ、パスワード、またはキー等の、証明書または他の類似認証メカニズムは、一般的に所有者だけに知らせることができる。従って、所有者による行為を不可能にする本人の死亡のような事象が発生した時、他の誰も、蓄積されている情報へのアクセスの方法を知らない場合、その情報は

永久的にロックアップされてしまう可能性がある

【発明の概要】本発明の特徴と利点は、所有者のバーチャルワレットに蓄積されている所有者の電子データを、安全に更新し、かつ管理するためのシステムと方法を提供することである。本発明の別の特徴と利点は、所有者のバーチャルワレットに蓄積されている所有者のデータに関連する技術が陳腐化したとき、これを更新するためのシステムと方法を提供することである。本発明の追加の特徴と利点は、所有者の死亡のような事象の発生時に、所有者のバーチャルワレットに蓄積されている所有者のデータにアクセスするためのシステムと方法を提供することである。本発明の更なる特徴と利点は、所有者の死亡時に、所有者のバーチャルワレットの内容を所有者の財産に利用できるようにするためのシステムと方法を提供することである。本発明の上記および他の特徴、利点、および目的を達成するために、本発明の実施形態は、所有者の機密データを安全に蓄積し、管理し、更新するためにの、そして所有者の死亡のような事象の発生時に、受託第三者が蓄積データにアクセスするためのシステムと方法を提供する。本発明の実施形態は、例えば少なくとも一部が所有者のパソコン上で、また少なくとも一部が銀行または同様の金融機関等の受託第三者のワレットサーバ上で実行されるバーチャルワレット・アプリケーションのようなアプリケーションソフトウェアを利用する。またバーチャルワレット・アプリケーションは、例えばバーチャル・エクゼキュータ機能とバーチャル・アーカイビスト機能（仮想的書庫）とを含む。本発明の実施形態において、データは、ネットワーク上のワレットサーバに結合されている所有者のパソコン等の端末で、所有者がバーチャルワレット・アプリケーション上にデータを入力することにより、あるいは電子メールメッセージ等の電子伝送による、商店や、弁護士など別の当事者からデータを所有者のために受け取ることにより、所有者のために蓄積される。ネットワークは、専用回線、またはインターネットのような公衆回線であることができる。所有者が入力し、バーチャルワレット・アプリケーションが所有者のために蓄積する機密情報のタイプは、例えば、識別情報、認証情報、証明書情報、アクセス・キー情報、ＰＩＮ番号情報、クレジットカード口座情報、デビットカード情報、銀行口座情報、および／または、遺言書情報、法的文書、保険証券、仲介手数料口座情報、デジタル無記名証券、デジタル株式券証書、およびデジタル公債証書のような他の個人情報を含む。本発明の実施形態は、種々のペイメント機能のための、そして所有者の機密データを蓄積するための、所有者用バーチャルワレットを設置することを含む。バーチャルワレット・アプリケーションは、蓄積データへの所有者によるアクセスのためのパスワード、機密キー、ＰＩＮ番号、またはこれに類するような機密装置を所有者へ自動的に割り当て、また例えばネットワーク上でワレットサーバに結合されている所有者の端末またはパソコンで、所有者へ機密装置に関する情報を自動的に送る。所有者の機密アクセス装置は、例えば２つの「フレーバ」または２つの局面、つまり所有者のアクセス局面と受託第三者のアクセス局面とを持つ。所有者のアクセス局面は、所有者に自動的に送られ、受託第三者のアクセス局面は、バーチャルワレット・アプリケーションのバーチャル・エクゼキュータ機能により自動的に蓄積される。本発明の実施形態では、機密装置の第三者のアクセス局面は、所有者の死亡または資格喪失等、所有者が行為を行えなくする影響を所有者に及ぼす事象の発生を条件とするバーチャルワレット・アプリケーションのバーチャル・エクゼキュータ機能により自動的にエスクローされる。所有者の、例えば、識別情報、認証情報、証明書情報、アクセス・キー情報、ＰＩＮ番号情報、およびパスワード情報などの機密アクセス情報は、バーチャルワレット・アプリケーションのバーチャル・エクゼキュータ機能により、所有者のために同様に自動的にエスクローされる。同様に、公開キー暗号手法インフラ、電子文書インフラ、デジタル署名インフラ、ユーザ名インフラ、パスワード・インフラ、指紋スキャナ・インフラ、および所有者の機密キー・インフラのような、種々の暗号解読インフラも、バーチャル・エクゼキュータ機能により、所有者のために自動的にエスクローされる。本発明の実施形態では、所有者の死亡または資格喪失のような事象の発生時に、所有者の財産のエクゼキュータまたは受託者等の所有者の代理人は、事象の発生および代理人の執行行為権限を確認するために必要とする、適切な文書を受託第三者に提示する。事象発生の確認は、所有者のバーチャルワレット・アプリケーションのバーチャル・エクゼキュータ機能に入力され、バーチャル・エクゼキュータ機能は、所有者の機密キーの受託第三者のアクセス局面のようなエスクローされた情報を用いて、所有者の蓄積データへのアクセスを自動的に提供する。また本発明の実施形態は、所有者のバーチャルワレットのバーチャルアーカイビスト機能(virchal archivist function) をも含み、この機能は蓄積データの技術局面を時々更新する。このバーチャル・アーカイビスト機能により更新される技術局面は、例えば文書署名のための技術、暗号化／暗号解読技術、文書署名のためのキーに関する技術、文書自体を読み出すことに関する技術、文書自体をアクセス可能にするのに用いられる変換ユーティリティに関する技術、および証明書取消しリストに関する技術を含む。バーチャル・アーカイビスト機能により更新される他の技術局面は、キー、デジタル証明書および公証人スタンプが文書自体に関連付けられた時間スタンプの日付現在で確実に有効であるようにするための確認と有効性の技術を含む。本発明の追加の目的、利点、および新規な特徴は、一部分は以下の説明で述べられており、また一部は以下の説明を吟味すれば、この技術に

精通する者には明らかだろうし、あるいは本発明を実施することにより学ぶことができよう。

【詳細な説明】一例が添付図面に図示されている本発明の一実施例形態を、ここで詳細に参照すると、本発明は、受託第三者により所有者の電子データを安全に蓄積し、更新し、管理するための、そして、所有者の死亡または資格喪失のような事象の発生時に、また蓄積データにアクセスするためのシステムと方法を提供する。図１は、本発明の実施形態のための、主要構成要素の概観および主要構成要素間の情報のフローを概略図的に示す。本発明の実施形態のためのシステムは、例えば所有者４のＰＣ２および銀行のような金融機関８のサーバ６の一方または両方に在住するバーチャルワレットのようなアプリケーションソフトウェアを利用する。図２は、本発明の実施形態のための、所有者が自らのバーチャルワレットに蓄積するデータのタイプの実施例を図解するテーブルである。図１と２を参照すると、所有者のＰＣ２に在住するバーチャルワレット１２のローカル局面（local aspect、ローカル部分）１０は、所有者４がインターネットのようなネットワーク１６上のワレットサーバ６に在住するバーチャルワレット１４全体への遠隔地からのアクセス権を獲得することを可能にする。ローカル局面１０は、ローカルワレットがサーバ６にオンラインでつながっているとき、ローカル局面からの最新情報を用いてバーチャルワレット１２のリモート局面１４（remote aspect、リモート部分）を更新する。バーチャルワレット１２中に所有者４のために蓄積されることができる情報のタイプは、例えば識別情報１８、認証情報２０、証明書２２、アクセス・キー２４、個人識別番号（ＰＩＮ）２６、クレジットカード口座情報２８、デビットカード情報３０、銀行口座情報３２、および、例えば所有者の、遺言書、法的文書、保険証券、仲介手数料口座情報、デジタル無記名証券、デジタル式株証書、およびデジタル公債証書のような個人情報を含む。更に図１を参照すると、証明書または、例えば通常は所有者４だけに知られている特定のＰＩＮ、パスワード、またはキー等の他の同様な認証メカニズム３６は、所有者のバーチャルワレット１２へ安全に蓄積されている所有者の電子データへのアクセス権を所有者が獲得することを可能にする。一般的に電子コマースに関連する、例えば公開キー暗号手法、電子文書、およびデジタル署名等のデジタルサービスのすべては、証明書を保持する人、またはワレットを所有する人が存在して、それらにアクセスすること、に依存している。所有者４が自らのパスワードを実際上、機密に保つ場合、それは、例えばユーザー名やパスワードと同程度に単純にすることができる。他方、例えば体温のある生身の指紋を取る指紋スキャナと同程度に複雑にするこもできる。所有者４が死亡すると、所有者の暗号解読インフラも同様に無くなり、事実上所有者と共にアクセス権もなくなる。本発明の実施形態のための、バーチャルワレット内の機能は、所有者４の死亡時、受託第三者、例えば銀行のような金融機関により開くことができるこの重大な情報の全てを有するファイルを維持することにより、問題に対する解決を提供する。これは、全ての口座の清算および所有者４の利害関係にある承継人による情報へのアクセスを可能にする。再び図１を参照すると、バーチャル・エクゼキュータ３８と呼ばれる本発明の実施形態のこの局面は、ひとたび所有者４が、例えば、死亡または法的に資格喪失したり、或いは他の事情により自らの用務を行なえなくなると、電子ワレット１２に蓄積されている所有者の安全な電子データへのアクセスを可能にする。このように、バーチャル・エクゼキュータ３８は、所有者４が、例えば、死亡または資格喪失したり、或いは他の事情により所有者自らが実行できなくなった後は、利害関係にある所有者の承継人へ渡されるべき所有者の安全な情報を提供する。本発明の実施形態のための、バーチャル・エクゼキュータ３８の機能は、キーおよび／または類似アクセス装置ないしはメカニズムをエスクローするサービスを提供し、それによって、所有者４が死亡したとき、キーは所有者の財産の一部となり、通常の財産清算の一部として処理できる。図３は、本発明の実施形態のための、バーチャル・エクゼキュータ３８によりエスクローされた情報のタイプの実施例を示すテーブルである。バーチャル・エクゼキュータ３８によりエスクローされた情報のタイプは、例えば識別情報１８、認証情報２０、証明書２２、アクセス・キー２４、ＰＩＮ番号２６、パスワード４０、および類似する他の機密アクセスメカニズム４２を含む。バーチャル・エクゼキュータ３８が無いと、例えば、認証情報２０、キー２４、特定ＰＩＮ２６、またはパスワード４０、により保護されている所有者の情報の全てが、一般的にバーチャルワレット１２に蓄積されている情報へのアクセス方法を知る一般的にはただ一人の所有者４の行為を行えなくなるとともに、永久にロックアップされる。本発明の実施形態では、所有者の機密キーおよび／または他の類似アクセス装置は、所有者４のための一種のバーチャル受託者であるバーチャル・エクゼキュータ３８を介して、例えば金融機関または銀行８である受託第三者によりエスクローされる。所有者４は、所有者の機密キーを受託第三者８にエスクローし、エスクローされたキーは所有者の財産の一部となる。換言すれば、エスクローされたキーは、所有者４が持つこともある所有者の遺言書、および全ての他の信託財産に似ている。例えば、所有者４は、所有者の親指の指紋解読を必要とする蓄積バリューまたはデジタルコイン等の、電子ファンドも持つことができる。所有者の死亡または資格喪失の事象の発生時に、本発明の実施形態のためのシステムと方法は、受託第三者８が、例えば、これらのコインが持つ価値へのアクセス権を得るための方法を提供する。本発明の実施形態のためのシステ

ムと方法は、例えば、ワレット内に蓄積されている所有者のバリュー等、バーチャルワレットの内容物へアクセスするために、バーチャルワレット１２に関連する技術インフラを提供する。バーチャルワレット１２に関連する技術インフラは、持続性のある、例えば２個の「フレーバ」を持つキーを提供する。図４は、本発明の実施形態のための、所有者のバーチャルワレット１２にアクセスするためのキー４４に関する２個の「フレーバ」の実施例を示すテーブルである。キーの第１フレーバは、所有者４がバーチャルワレット１２へのアクセスのために毎日用いるのに必要な所有者の機密アクセスメカニズム３６である。キーの第２フレーバは、バーチャルワレット１２への第三者アクセス権を与えるために、受託第三者８により保持される。第２フレーバ４６は、ひとたび所有者４が、所有者の主アクセス装置３６を使用できなくなると、所有者のバーチャルワレット１２の内容物への受託第三者８のアクセス権を与える、事実上、マスタ・キーのようなものである。図５は、本発明の実施形態のための、図１に示す情報のフローを強調してあり、また所有者の蓄積データをエスクローしてそれにアクセスするプロセスに関する更なる詳細を提供する。Ｓ１で、所有者４が、所有者のＰＣ２のような端末でバーチャルワレット１２を設定する。Ｓ２で、所有者は、ワレットへの所有者のアクセス権を与える新しいキー３６を自動的に受け取る。Ｓ３で、そのキーを使ってスタートすると、キー・エスクローが、バーチャルワレット１２内のバーチャル・エクゼキュータ機能３８により、受託第三者８とともにに自動生成される。バーチャル・エクゼキュータ機能３８は、キー３６が適切にエスクローされることを自動的に確実にする。所有者４の死亡のような事象が発生した時、所有者の個人代理人が、死亡証明書のような所有者の死亡に関する適切な通知を、Ｓ４で受託第三者８に提示すると、バーチャル・エクゼキュータ３８は、所有者が実際に死亡していることを確信する。Ｓ５で、バーチャル・エクゼキュータ３８は、自らのキー・セットを用いて、所有者４がこれらのキーにより保護してきた内容物の全てを、財産として利用できるようにする。例えば、それらが所有者のバーチャルワレット１２内のデジタルファンドへの所有者のアクセス権である場合、これらのキーのうちの１つが、これらのファンドへのアクセスを許す。本発明の実施形態において、機密キーに加え、所有者４は、バーチャルワレット１２内に蓄積されている種々の他の情報、例えば所有者の遺言書３４を持つこともできる。所有者４は、例えば、所有者のバーチャルワレット１２に関連するデータアーカイブ内に、所有者の遺言書３４の電子コピーを遺言書の正式コピーとして蓄積しておくこともできる。再び図５を参照すると、所有者４の死亡時に、所有者の個人代理人は、個人代理人の権限を証明書するために、適切な死亡証明書および／または他のしかるべき文書のコピーをとり、その文書を受託第三者８の面前で提示する。バーチャル・エクゼキュータ３８が所有者の死亡を確信すると、Ｓ５で、バーチャル・エクゼキュータは、同様に、キー・セットを用いて、所有者の蓄積されている遺言書３４が所有者の財産として利用できるようにする。所有者の死亡時に、所有者の死亡と、受託第三者に対して行為を行う所有者の個人代理人の権限とを証明してそれらを文書化することは、本発明の実施形態のセキュリティメカニズムの一部である。本発明の更なる局面は、バーチャル・アーカイビストと呼ばれるバーチャルワレット１２内の機能である。バーチャル・アーカイビストは、例えば蓄積情報に関連する種々の技術が陳腐化したとき、バーチャルワレット内に蓄積されている電子情報へのアクセスと、その情報の更新に備える。図６は、本発明の実施形態のための、バーチャル・アーカイビストにより更新される技術のタイプの実施例を示すテーブルである。バーチャル・アーカイビスト４６は、技術の変化に適合させるために、例えば文書への署名４８、文書暗号化／暗号解読５０、キー５２、文書自体の読出し５４、文書自体をアクセス可能にするために用いられるファイル変換ユーティリティ５５、および証明書取消しリスト５６等の技術を更新する。バーチャル・アーカイビスト４６は、キー５２、デジタル証明書５７、および公証人スタンプ６０が、それら文書自体に関連する時間スタンプの日付５８現在で確実に有効にするための、確認／有効性の技術も更新する。更に、本発明の実施形態において、バーチャル・アーカイビスト４６は、陳腐化した技術で情報を取り出し、オリジナル情報の完全性を維持しながら最新技術と両立するようにその情報を更新する。従ってバーチャル・アーカイビスト４６により、全ての情報を最新の技術進歩に適合させることができる。例えば、電子文書は、実際上オリジナル文書となるので、所有者のバーチャルワレット１２のデータ・アーカイブ部分へ電子的に蓄積されている所有者の遺言書３４は、所有者の正式な遺言書になる。現時点で書かれる所有者の遺言書は、ＷｉｎｄｏｗｓＮＴ４．０のようなオペレーティングシステムを用いて、Ｉｎｔｅｌ Ｐｅｎｔｉｕｍコンピュータ上で実行されるＷｏｒｄ７．０のようなアプリケーションを用いて書かれるだろう。所有者が将来、もっと後になって死亡するような場合、Ｗｏｒｄ７．０のコピー、Ｉｎｔｅｌコンピュータ、またはＮＴ４．０のコピーを容易に利用できるとは考えられない。従って、所有者４が将来死亡したとき、所有者の遺言書が過去に署名されて暗号化されるとともに保護され、また所有者が全てのキーを蓄積して保存していて、バーチャル・エクゼキュータがそれらへのアクセス権を持っているという事実があっても、アクセスメカニズムが提示されないので、ファイルを読むことはできないだろう。本発明の実施形態では、バーチャル・アーカイビスト４６は、事実上、責任負担機能である。所有者のフ

15

ァイルは、所有者のバーチャルワレット１２に関連するデータ・アーカイブに保存されているので、バーチャル・アーカイビスト４６は、時を経て技術が変化するとともに、蓄積データおよびデータに関連する技術を自動的に更新することにより、長い年月に渡りファイルへのアクセスが可能になるように、蓄積されたファイルを維持する。バーチャル・アーカイビスト４６は、個人情報アーカイブであるバーチャルワレット１２内の機能のうちの１つの一部である。所有者４は、バーチャルワレット１２に関連するデータ・アーカイブに所有者のデータを入力するので、バーチャルアーカイビスト４６は、所有者のデータがどんなものかを知らされ、データを自動的にフォーマットするので、データは継続して利用される。本発明の好ましい種々の実施形態が、本発明の種々の目的を達成する中で説明されている。これらの実施形態は、本発明の原理の例示であることを認識されたい。本発明の精神と範囲を逸脱しない発明の多くの変形や適合があり得ることは、この技術に精通する者には容易に明らかになろう。よって、本発明は以下の請求項によってのみ限定される。

16

【図面の簡単な説明】

【図１】図１は、本発明の実施形態のための、主要構成要素の概観および主要構成要素間の情報の流れを概略的に示し；

【図２】図２は、本発明の実施形態のための、所有者が自らのバーチャルワレットに蓄積するデータのタイプの実施例を示すテーブルであり；

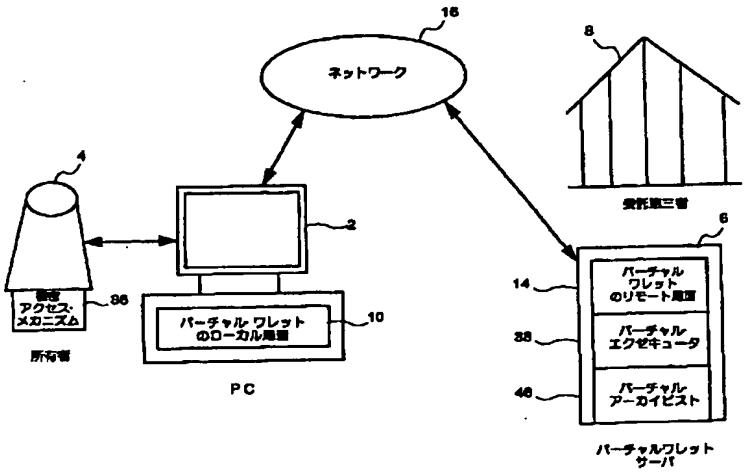
【図３】図３は、本発明の実施形態のための、バーチャル・エクゼキュータによりエスクローされた情報タイプの実施例を示すテーブルであり；

【図４】図４は、本発明の実施形態のための、所有者のバーチャルワレットへのアクセス用キーに関する２つの「フレーバ」の実施例を示すテーブルであり；

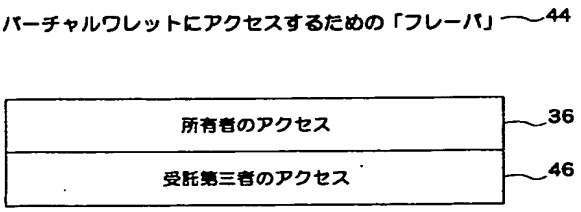
【図５】図５は、本発明の実施形態のための、図１に示す情報のフローを強調してあり、所有者の蓄積データをエスクローし、またこれにアクセスするプロセスに関して更に詳細な説明を提供するフローチャートであり；

【図６】図６は、本発明の実施形態のための、バーチャル・アーカイビスト機能により更新される技術のタイプの実施例を示すテーブルである。

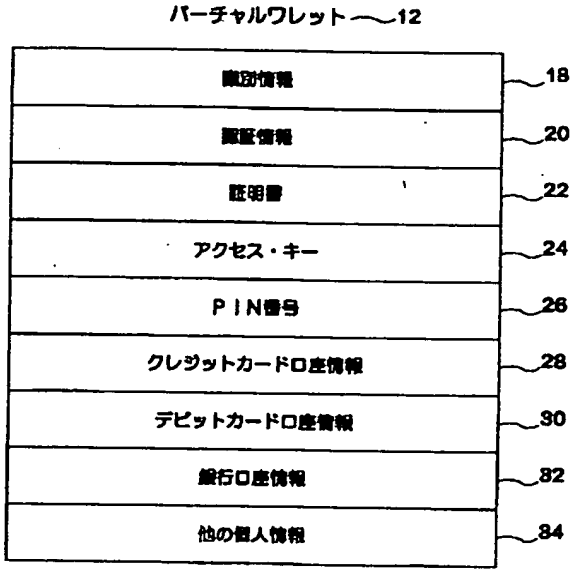
【図１】



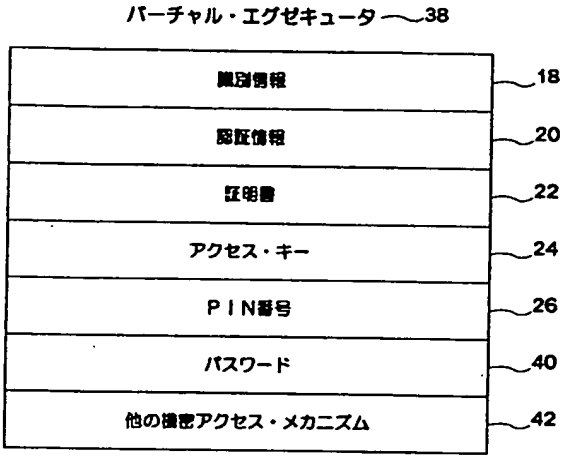
【図４】



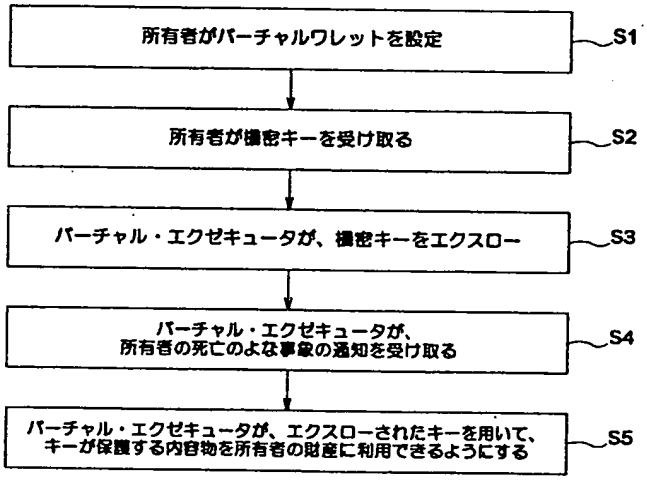
【図２】



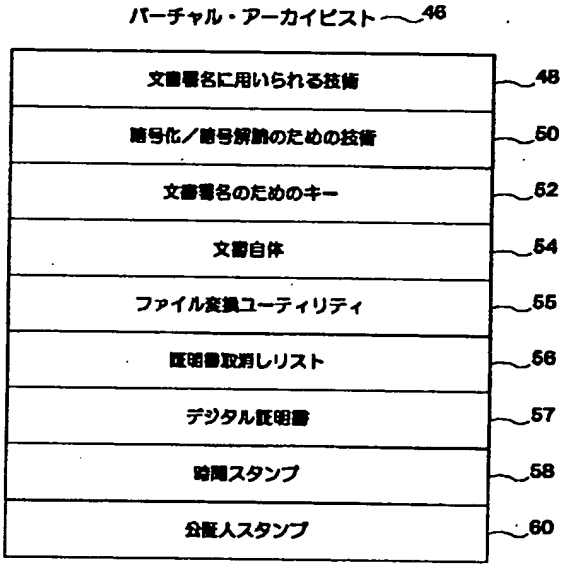
【図３】



【図５】



【図６】



フロントページの続き

(71)出願人 598156527
12731 W. Jefferson Boulevard, Los Angeles, California 90066, U. S. A.
(72)発明者 クリス ティ. パルテンゲ
アメリカ合衆国 カリフォルニア州 91326, ノースリッジ, エントレイド アヴェニュー 11718
(72)発明者 アルノール ビィ. マムダーニ
アメリカ合衆国 カリフォルニア州 90291, ヴェニス, ペンマーアヴェニュー 2030
(72)発明者 リサ エズロル
アメリカ合衆国 ニューヨーク州 10021, ニューヨーク, イースト セブンティ セカンド ストリート, アパートメント 42 A, 525